ДОНБАСЬКА ДЕРЖАВНА МАШИНОБУДІВНА АКАДЕМІЯ

Затверджую:

Перший проректор _____А.М. Фесенко

“____”_____2018 р.

РОБОЧА НАВЧАЛЬНА ПРОГРАМА

ДИСЦИПЛІНИ

ІНФОРМАЦІЙНА БЕЗПЕКА В КОМП’ЮТЕРНИХ МЕРЕЖАХ

для спеціальності

123 – «Комп’ютерна інженерія»
(шифр, напрямів, спеціальностей)

(денна форма навчання)

Ухвалено методичною комісією факультету АМ	Програму рекомендовано кафедрою АВП
Протокол № ____ від_____	Протокол №_____ від_____
Голова МК	Завідувач кафедри АВП
_____В.Г. Макшанцев (підпис, ініціали, прізвище)	_____Г.П. Клименко (підпис, ініціали, прізвище)

Краматорськ 2018

Повна назва: Інформаційна безпека в комп'ютерних мережах

Статус: Дисципліна вільного вибору

Мета: Багатоаспектний розгляд означеного поняття захисту інформації в комп’ютерних системах з позицій інтересів користувачів, програмістів, операторів, експлуатаційників, адміністраторів обчислювальних систем.

Обсяг, методики, і технології викладання дисципліни:

Тематичний план дисципліни «Інформаційна безпека в комп'ютерних мережах» в магістратурі спеціальності 123 «Комп’ютерна інженерія» складається з трьох модулів, кожен з яких поєднує в собі відносно окремий самостійний блок дисципліни, який логічно пов'язує кілька навчальних елементів дисципліни за змістом і взаємозв'язками.

Для визначення рівня засвоєння слухачами навчального матеріалу використовуються такі форми та методи навчання:

1) лекційні заняття, на яких викладається теоретичний матеріал, наводяться практичні приклади; заняття проводяться з використанням технічних та програмних засобів;

2) лабораторні заняття, що передбачають підготовку теоретичних та практичних питань з вивчення критеріїв, методів та засобів забезпечення інформаційної безпеки, шляхи запобігання комп’ютерним інцидентам;

3) консультації, які проводяться з метою допомоги студентам у виконанні їх самостійних завдань та роз’яснення окремих розділів теоретичного матеріалу, відпрацювання студентами пропущених занять.

Знання та навички: студенти повинні:

знати:

- міжнародні та державні нормативно-правові засади захисту інформації в комп’ютерних системах;

- основні загрози інформації та можливі шляхи реалізації НСД зловмисником;

- основні положення по формуванню структури системи захисту

інформації на підприємстві (установі, організації);

- організаційно-методичне забезпечення системи захисту інформації;
- особливості обробки конфіденційної інформації в автоматизованих системах;
- основні напрями і складові КСЗІ на об'єктах інформатизації;
- основи теорії криптографії та криптоаналізу, типи шифрувальних алгоритмів та спеціалізованих програм і характеристики обладнання для техзахисту;
- основні уразливості механізмів безпеки сучасних операційних систем (ОС), та їх порівняльний аналіз;
- засоби реалізації атак на протоколи;
- методи та інструментальні засоби реалізації програмних атак;
- основи безпечної міжмережевої взаємодії і підключення до глобальних телекомунікаційних мереж.

термінологію локальних та глобальних мереж;

вміти:

- організовувати і забезпечувати захист інформації в приміщеннях з комп’ютерної технікою і каналах зв'язку;
- аналізувати вразливості, створювати моделі загроз в автоматизованій системі;
- організовувати і забезпечувати захист інформації засобами криптографії та антивірусного захисту;
- діагностувати, протидіяти та попереджати атаки на паролі, засоби автоматичної генерації, перехвату та викриття паролів;
- діагностувати, протидіяти та попереджати атаки на служби і протоколи інформаційного обміну; засоби реалізації атак на протоколи;
- організовувати і забезпечувати захист інформації управлінням доступу до ресурсів автоматизованої системи на базі ОС Windows;
- створювати та реалізовувати політики інформаційної безпеки штатними засобами основних операційних систем;

- реалізовувати політики безпеки засобами резервного копіювання, попередження втрати даних і безперебійного живлення;
- створювати типові рішення по захисту корпоративної мережі в умовах несанкціонованого доступу за допомогою спеціальних програмних і технічних засобів, використовуючи процедури дистанційної реєстрації подій, резервування даних на сервері, перевірки захищеності комп'ютера і паролів, контроль змін в системних файлах, систему аутентифікації тощо.

Кількість годин (кількість кредитів ЄКТС): На вивчення навчальної дисципліни відводиться 90 години / 3кредити.

Види робіт: Контроль за рівнем засвоєння матеріалу та знань студентів проводиться у таких формах: виконання лабораторних робіт; самостійне опрацювання теоретичного матеріалу, поточне опитування під час лекційних занять; залік.

Протягом триместру здійснюється поточний та підсумковий контроль. Поточний контроль здійснюється під час захисту лабораторних робіт, перевірки самостійної роботи, надання відповідей біля дошки, перевірки виконаних творчо-пошукових завдань. Підсумковий контроль з дисципліни «Захист інформації в комп'ютерних системах» проводиться відповідно до навчального плану у вигляді заліку у 11-му триместрі, в терміни, встановлені графіком навчального процесу та в обсязі навчального матеріалу.

Оцінювання:

Форма контролю	Сума балів за семестр
Захист лабораторних робіт	55
Опитування на лекційних заняттях	5
Самостійна робота	10
Загальна кількість балів за семестр	**70**
Залік	30
Всього за триместр	**100**

Структура навчальної дисципліни:

№ з/п	Назви розділів та тем	Всього годин	За формами занять, годин				
			Аудиторні				СРС
			Лек.	Сем.	ЛР	ПР	
ЗМІСТОВИЙ МОДУЛЬ 1. ***Теоретичні засади захисту інформації в комп'ютерних мережах***							
1	Законодавчі аспекти захисту інформації - міжнародні та державні	4	2				2
2	Інформаційна безпека комп'ютерних систем. Шляхи витоку інформації та способи резервування інформації	6	2			1	3
ЗМІСТОВИЙ МОДУЛЬ 2. ***Програмно-апаратне забезпечення системи безпеки***							
3	Комп'ютерні віруси та антивірусні програми	8	2			2	4
4	Загальна характеристика криптології. Шифротехнології. Криптосистеми.	8	2			2	4
5	Методи і засоби вбудови скритої службової інформації в аудіо - та відеосигнали. Поняття стеганографії.	8	2			2	4
6	Реалізація політики безпеки штатними засобами основних операційних систем, сучасних СУБД та програмно-апаратних комплексів	12	4			2	6
ЗМІСТОВИЙ МОДУЛЬ 3. ***Безпека сучасних мережевих технологій***							
7	Побудова системи захисту корпоративних мереж на основі застосування міжмережевих екранів і VPN рішень. Протокол SSH як засіб шифрування трафіку.	12	4			2	6
8	Виявлення і протидія програмним атакам в корпоративних мережах.	12	4			2	6
9	Політика безпеки при роботі у відкритих мережах в глобальній мережі Інтернет.	10	4			1	5
10	Комплексна система захисту інформації підприємства, організації, установи	10	4			1	5
Всього за 8-й триместр		**90**	**30**			**15**	**45**

Розробник програми:

к.т.н., доцент Сус С.П.